Data Storage Media Protection and Personal Assets

The portable nature and small size of mobile storage devices make them convenient to utilize for the purposes of storing data. However, such devices are highly susceptible to loss and/or theft, thus, increasing the likelihood of data compromise. Note: Such media include, but are not limited to, USB drives, cell phones, personal digital assistants, and digital music players owned by employees, contractors, and students. The COV has recognized the increased security risks associated with the use of such devices and has instituted the following requirement for all COV agencies: Section 6.2.2, item 4, of the COV ITRM SEC 501-01, states that [the agency] prohibit the connection of any mobile data storage media not owned by COV to any COV IT system and storage of COV data on any mobile data storage media not owned by COV. Additional risks associated with the use of such devices include but are not limited to:

- Users intentionally or unintentionally installing or downloading malicious code or software from unreliable sources potentially increasing the risk of exposure to exploits such as viruses, worms, spy-ware, keystroke loggers, phishing software and Trojan horses on campus computers, servers, and on the Commonwealth of Virginia (COV) network.
- Users intentionally or unintentionally installing unlicensed software
- Users intentionally or unintentionally installing unapproved patches that could compromise the stability of the system
- Potential to store sensitive information on the storage device unencrypted, which could lead to loss of such information.

In lieu of the associated risks, TNCC has implemented the following mitigating controls:

- Restricted functionality of the classroom and lab computers through the use of group policies and installed the Deep Freeze application. Deep Freeze restores the computer to its original state after a user logs off.
- Network segmentation, in which classroom computers are in a demilitarized zone (DMZ) which isolates and prevents them from connecting to the college’s administrative network.
- Network Access Control (NAC) that verifies AV, patches, and updates; the NAC prevents users from accessing the network until user AV, patches, and updates are current.
- Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) solutions and a Checkpoint firewall.

The college must ensure that appropriate steps are taken with respect to the handling, storage, and protection of confidential sensitive student, faculty, staff, and college data on non-COV owned equipment. Confidential sensitive data is personally identifiable information that is protected by law (local, state, or federal) and requires the highest level of protection. If compromised, such data could potentially be subject to misuse, improper disclosure, or identity theft. Examples of confidential sensitive data includes but is not limited to social security numbers, financial information, credit card numbers, personal addresses, driver's license...
numbers, etc. To this end, in order to ensure compliance with this requirement, TNCC prohibits the following:

- The connection of any personally owned mobile storage media or non-COV owned storage media to any COV IT system
- Storing confidential sensitive student, faculty, staff, college data on mobile data storage media not owned by COV

Employees should utilize their home directory (H: drive) to save data. Saving the information to the H: drive will allow users to access their data when logging onto any campus computer.

TNCC will allow students to utilize personally owned mobile storage devices to connect to classroom computers, in recognition of the need for students to save data for instructional purposes. Additionally, faculty, and instructional assistants, may use personally owned mobile storage devices for instructional purposes to connect to classroom and lab computers. The intent of this policy would not undermine the COV ITRM SEC 501-01 policy due to the following mitigating controls:

- TNCC has restricted functionality of the classroom computers through the use of group policies and installed the Deep Freeze application. Deep Freeze allows students to do the work necessary for instructional purposes and restores a computer to its original state after a user logs off.
- TNCC classroom computers are in a DMZ, which prevents them from connecting to the college’s administrative network

President’s Signature: ___________________________________________ Date: ______________

VP of IT Signature: ___________________________________________ Date: ______________

College ISO Signature: _________________________________________ Date: ______________